## A. Distribution-of-primes result #2:

**Theorem 1.13.**

$$\sum_{m=1}^{\infty} 1/p_m \text{ diverges.}$$

**Proof.**

positive integers

Spz not: then $\exists\, k \in \mathbb{Z}_+$ with

$$\sum_{m=k+1}^{\infty} 1/p_m \leq 1/2. \qquad (*)$$

We'll derive a contradiction, as follows.
Let $Q = p_1 p_2 \cdots p_k$. We'll show that

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left( \sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t. \qquad (**)$$

The left side diverges by the integral test.
But by $(*)$, the right side is

$$\leq \sum_{t=1}^{\infty} \frac{1}{2^t} < \infty.$$

Contradiction. So our theorem must be true.

To prove $(**)$ note that, if we expand out

$$\left( \sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t,$$

then every integer that's a product of exactly $t$ (not necessarily distinct) primes $p_m$, with $m \geq k+1$, appears as a denominator.

(Example:

$$\left(\sum_{m=5}^{\infty}\frac{1}{p_m}\right)^3 = \left(\frac{1}{11}+\frac{1}{13}+\frac{1}{15}+\cdots\right)^3$$

$$= \frac{1}{11^3}+\frac{1}{13^3}+\frac{1}{15^3}+\frac{1}{11^2\cdot 13}+\frac{1}{11^2\cdot 15}+\frac{1}{13^2\cdot 15}+\cdots)$$

But for any $n\in\mathbb{Z}_+$, $1+nQ$ is such a product, for some $t\in\mathbb{Z}$, since $1+nQ$ is relatively prime to those $p_m$'s with $1\le m\le k$. (Each of the latter $p_m$'s divides $Q$ but not $1$.)

Conclusion: each summand on the left side of $(**)$ appears as a summand in the expansion of the right side.

But all of these summands are non-negative, whence $(**)$ holds, whence our contradiction, whence our theorem.

□

B. The Euclidean algorithm.

This is a method for determining $(a,b)$ without needing the prime factorizations of $a$ and $b$.

<u>Lemma</u>: the division algorithm (= Thm. 1.14).

If $a$ and $b$ are integers and $b>0$, then $\exists$ a unique pair of integers $q$ and $r$ such that

$$a = bq + r \quad\text{and}\quad 0\le r<b.$$

**Proof**

Given such $a$ and $b$, let
$$S = \{a - bx : x \in \mathbb{Z} \text{ and } a - bx \geq 0\}$$

By the well-ordering property of $\mathbb{N}$ (the natural numbers), $S$ has a least element

$$r = a - bq. \qquad (*^3)$$

Then certainly $a = bq + r$. Also, $r \geq 0$ since $r \in S$ by definition.
To show that $r < b$, suppose not. Then

(i) $r - b \geq 0$,
(ii) $r - b = a - b(q+1)$ by $(*^3)$,
(iii) $r - b < r$ (since $b > 0$).

That is, $r - b$ is an element of $S$ that's less than $r$, contradicting the minimality of $r$.

So the desired $q$ and $r$ exist. Uniqueness is an exercise. ∎

Now suppose we want to find $(264, 2520)$.

We divide $r_1 = 264$ into $r_0 = 2520$, using the division algorithm:

$$\underbrace{2520}_{r_0} = \underbrace{264}_{r_1} \cdot 9 + \underbrace{144}_{r_2}$$

Next, divide $r_2 = 144$ into $r_1 = 264$:

$$\overset{r_1}{264} = \overset{r_2}{144} \cdot 1 + \overset{r_3}{120}$$

Divide $r_3$ into $r_2$:

$$\overset{r_2}{144} = \overset{r_3}{120} \cdot 1 + \overset{r_4}{24}$$

Divide $r_4$ into $r_3$:

$$\overset{r_3}{120} = \overset{r_4}{24} \cdot 5 + \overset{r_5}{0}$$

Since $r_5 = 0$, we conclude that $r_4 = (r_0, r_1)$, i.e. $24 = (264, 2520)$.

In general, divide $r_0 = b$ into $r_1 = a$, then divide the remainder $r_2$ into $r_1$; divide the new remainder $r_3$ into $r_2$, ... stop when $r_{n+1} = 0$. Then $r_n = (r_1, r_2)$. This is the <u>Euclidean algorithm</u> (= Thm. 1.15.)

It works in general because we have a sequence of steps

$$r_{i-1} = r_i q_i + r_{i+1}, \qquad 0 \le r_{i+1} < r_i.$$

The fact that the $r_i$'s are decreasing and $\ge 0$ means eventually $r_i = 0$. Say $r_{n+1} = 0$: then by induction, we show that (a) $r_n | r_1$ and $r_n | r_0$; (b) $r_n = r_0 x + r_1 y$ for $x, y$ integers. So

$$r_n = (r_0, r_1) = (a, b).$$